2132

IN THE

UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANTS:	PAUL C. KOCHER et al.
SERIAL NO.:	10/005,105
FILING DATE:	December 03, 2001
TITLE:	DIFFERENTIAL POWER ANALYSIS METHOD AND APPARATUS
EXAMINER:	not yet known
CONFIRMATION NO:	1675
GROUP ART UNIT:	2132
ATTY. DKT. NO.:	44424162-8721

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop AMENDMENT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below:

Dated: 22 September 2004 By: Michael C. Martensen

Michael C. Martensen, Reg. No. 46,901

MAIL STOP AMENDMENT
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

SIR:

Pursuant to the provisions of 37 CFR 1.56 and 1.97-1.98, Applicants hereby cite the references listed on the accompanying substitute PTO-1449 without inferring or suggesting, but instead expressly disclaiming any inference or suggestion, that any more pertinent reference exists. The filing of the information disclosure statement shall not be construed as a representation that a search has been made (37 CFR §1.97(g)), or an admission that the

information cited is, or is considered to be, material to patentability. Applicants enclose herewith copies of the all cited references. All references are in the English language.

The Commissioner is authorized to charge any fees required in connection with the submission of this IDS to deposit account number 19-3140. This sheet is being submitted in duplicate.

Respectfully submitted,

22 February 2002

Michael C. Martensen
Registration No. 46,901
Attorney under Rule 34(a)

SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. Box 061080
Wacker Drive Station, Sears Tower
Chicago, IL 60606-1080
Tel.: (415) 882-0357

enclosures

PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 3

Complete if Known	
Application Number	10/005,105
Filing Date	December 3, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	not yet known
Attorney Docket Number	44424162-8721

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	AA	US-4,203,166	05/13/1980	Ehrsam et al.	
	AB	US-4,214,126	07/22/1980	Wipff	
	AC	US-4,243,890	01/06/1981	Miller et al.	
	AD	US-5,241,598	08/31/1993	Raith	
	AE	US-5,297,201	03/22/1994	Dunlavy	
	AF	US-5,341,423	08/23/1994	Nossen	
	AG	US-5,369,706	11/29/1994	Latka	
	AH	US-5,412,379	05/02/1995	Waraska et al.	
	AI	US-5,420,925	05/30/1995	Michaels	
	AJ	US-5,544,086	08/06/1996	Davis et al.	
	AK	US-5,552,776	09/03/1996	Wade et al.	
	AL	US-5,559,887	09/24/1996	Davis et al.	
	AM	US-5,600,324	02/04/1997	Reed et al.	
	AN	US-5,633,930	05/27/1997	Davis et al.	
	AO	US-5,733,047	03/31/1998	Furuta et al.	
	AP	US-5,761,306	06/02/1998	Lewis	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Number Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
	AQ	EP 0 529 261 A2	03/03/1993	IBM Corp.		☐
	AR	EP 0 582 395 A2	02/09/1994	Digital Equipment Corp.		☐
						☐
						☐
						☐

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unqiue citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 2 of 3

Complete if Known	
Application Number	10/005,105
Filing Date	December 3, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Not yet know
Attorney Docket Number	44424162-8721

RECEIVED
SEP 2 7 2004
Technology Center 2100

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	AS	US-5,778,065	07/07/1998	Hauser, et al.	
	AT	US-5,796,836	08/18/1998	Markham, Thomas R.	
	AU	US-5,995,629	11/30/1999	Reiner	

OIPE
SEP 24 2004
PATENT & TRADEMARK OFFICE

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Number Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
						☐
						☐
						☐
						☐
						☐

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unqiue citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Please type a plus sign (+) inside this box ™ [+]

Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 3 of 3

Complete if Known	
Application Number	10/005,105
Filing Date	December 3, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	not yet known
Attorney Docket Number	44424162-8721

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	CiteNo.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	AV	American National Standards for Financial Services, secretariat - American Bankers Association (ANS/ABA x9.24-1997), "Financial Services Key Management," approved April 6, 1992, American National Standards Institute; pgs. 1-71	
	AW	JUENEMAN, Robert R., "Analysis of Certain Aspects of Output Feedback Mode", Satellite Business Systems, 1998; pgs. 99-127	
	AX	BAUER, Friedrich L., "Cryptology - Methods and Maxims", Technical University Munich, 1998; pgs. 31-48	
	AY	CONNOR, Doug (Technical Editor), "Cryptographic Techniques - Secure Your Wireless Designs", 01/18/96; pgs. 57-68	
	AZ	HORNAUER et al., "Markov Ciphers and Alternating Groups," Eurocrypt 91, 1991; pgs. 453-460	
	BA	KOBLITZ, "A Course in Number Theory and Cryptography" 2e, 1994, Chapter III; pgs. 53-77	
	BB	LAI et al., "Markov Ciphers and Differential Cryptanalysis," Eurocrypt 91, 1991; pgs. 17-38	
	BC	HACHEZ et. al. "Timing Attack: What Can Be Achieved By A Powerful Adversary?" 1999	
	BD	KOCHER, Paul C., "Cryptanalysis of Diffie-Hellman, RSA, DSS, and Other Systems Using Timing Attacks," Report 7 December 1995; pgs. 1-6	
	BE	KALISKI, Burt, "Timing Attacks on Cryptosystem," RSA Laboratories, Bulletin, Number 2, January 23, 1996	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Unique citation designation number. [2] Applicant is to place a check mark here if English language Translation is attached.